IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Cuomo et al.**

Serial No.: **09/627,373**

Filed: **July 28, 2000**

For: **Method and Apparatus for Securing Session Information of Users in a Web Application Server Environment**

§ Group Art Unit: **3621**

§

§ Examiner: **Backer, Firmin**

§

§ Attorney Docket No.: **RSW9-2000-0089-US1**

§

Certificate of Mailing Under 37 C.F.R. § 1.8(a)

I hereby certify this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on November 18, 2003.

By: Rebecca Clayton

Rebecca Clayton

36736

PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appellant's Brief (in triplicate) (37 C.F.R. 1.192); and
- Our return postcard.

A fee of $330.00 is required for filing an Appellant's Brief. Please charge this fee to IBM Deposit Account No. 09-0461. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to Deposit Account No. 09-0461. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to Deposit Account No. 09-0461.

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
CARSTENS, YEE & CAHOON, LLP
P.O. Box 802334
Dallas, Texas 75380
(972) 367-2001
ATTORNEY FOR APPLICANTS

Docket No. RSW9-2000-0089-US1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Cuomo et al.** §

Serial No. **09/627,373** §

Filed: **July 28, 2000** §

For: **Method and Apparatus for Securing Session Information of Users in a Web Application Server Environment** §

§ Group Art Unit: **3621**

§ Examiner: **Backer, Firmin**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

Certificate of Mailing Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on November 18, 2003.

By: Rebecca Clayton
Rebecca Clayton

APPELLANT'S BRIEF (37 C.F.R. 1.192)

This brief is in furtherance of the Notice of Appeal, filed in this case on September 19, 2003.

The fees required under § 1.17(c), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. 1.192(a))

11/25/2003 AWONDAF1 00000081 090461 09627373
01 FC:1402 330.00 DA

REAL PARTIES IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interference's that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interference's.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-63

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 1-8, 18-21, 30-37, 47-50, 59, 61
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 9-17, 22-29, 38-46, 51-58, 60, 62 and 63
4. Claims allowed: none
5. Claims rejected: 9-17, 22-29, 38-46, 51-58, 60, 62 and 63

C. CLAIMS ON APPEAL

The claims on appeal are: 9-17, 22-29, 38-46, 51-58, 60, 62 and 63

STATUS OF AMENDMENTS

An amendment after final requesting reconsideration of the final claim rejection was filed on July 21, 2003, and was not deemed persuasive by the Examiner.

SUMMARY OF INVENTION

An improved data processing security system. In addition to performing traditional client authentication when a client requests access to a resource - where a server determines whether a client's presented credentials are valid - the client's credentials are also compared with a data structure associated with the particular session prior to granting access to what is being requested by the client.

The detailed description of the preferred embodiment is shown in Appellants's Figure 5A and Figure 5C, and described at Specification page 15, line 22 – page 16, line 17 and page 17, line 16 – page 18, line 17. In particular, a client initiates a request that requires authentication at step 502 (Figure 5A) and submits the request along with credentials to a server, which checks authentication at step 508 (Figure 5A). If authentication is successful in step 510 (Figure 5A), the server generates a session ID at step 514 (Figure 5A) and fulfills the request. This establishes the session between the client and server. Once the session is established, subsequent client requests are processed in the preferred embodiment according to the flow chart shown in Figure 5C. The client initiates a request at step 542 (Figure 5C) and submits the request along with the session ID and credentials to the server. The server checks the credentials at step 544 (Figure 5C). If the credentials are valid, a determination is made as to whether the session ID is valid at step 550 (Figure 5C). If the session ID is valid at step 550 (Figure 5C), the server retrieves the session object at step 554 (Figure 5C), compares the received credentials with the credentials in the retrieved session object at step 556 (Figure 5C), and determines whether these credentials match at step 558 (Figure 5C). If the credentials do match, the server fulfills the request at step 562 (Figure 5C) and the client may access content at step 564 (Figure 5C). Thus, not only does the server authenticate the client, but credentials associated with a session are also used to determine/compare with client credentials prior to granting client access - and therefore an improved data processing security system is provided.

ISSUES

A. Whether Claims 22-29 and 51-58 were properly rejected by the Examiner under 35 U.S.C. 102(b) as being unpatentable over Dustan et al. (U.S. Patent 5,884,312).

B. Whether Claims 9-17, 38-46, 60 and 63 were properly rejected by the Examiner under 35 U.S.C. 103 (a) as being unpatentable over Dustan et al. (U.S. Patent 5,884,312) in view of Shi et al. (U.S. Patent 5,875,296).

C. Whether Claim 62 was properly rejected by the Examiner.

GROUPING OF CLAIMS

Group I Claims 22-29 and 51-58

Group II Claims 9-17, 38-46, 60 and 63

Group III Claim 62

ARGUMENT

A. Appellants will now show that the claims of Group I have been erroneously rejected under 35 U.S.C. 102(b) as every element of the claimed invention is not identically shown in a single reference.

For a prior art reference to anticipate in terms of 35 U.S.C. 102, every element of the claimed invention must be identically shown in a single reference. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990). Appellants show that every element of the claimed invention is not identically shown in the cited Dustan et al. reference, as such reference does not teach the claimed steps of "retrieving a session data structure including a second credential in response to the session identification being valid", or "determining whether the first credential and the second credential match". In rejecting Claim 22, the Examiner merely states that "Dustan et al teach that the session id is also verified, column 9, lines 27-30". This cited Dustin passage is reproduced in its entirety below:

> "Generally, though, database server 22 will verify the session id, check to ensure that the client has not waited too long between requests, and will log all requests made by the user in an activity log table."

Appellants show that in addition to claiming "determining whether the session identification is valid", Claim 22 also recites "retrieving a session data structure including a second credential in response to the session identification being valid" and "determining whether the first credential and the second credential match". As can be seen, the claim recites that responsive to the session identification being valid, a session data structure is retrieved. This session data structure includes a second credential and a determination is made – in addition to determining whether the session identification is valid – whether a received first credential matches the second credential, the second credential being a part of the session data structure that is retrieved responsive to the session identification being valid. The cited reference does not teach, nor has the Examiner alleged a teaching of, these claimed steps of retrieving a session data structure responsive to the second identification being valid and determining whether the first credential

and the second credential match, and hence it is shown that Claim 22 and thus Group I has been erroneously rejected under 35 U.S.C. 102(b).

This can also be seen at Dustin's Figure 6, where after a received session id is determined to be correct at steps 236 and 238, the function requested by a user is compared with user permissions/rights that are stored in a user table to determine if the user has sufficient privileges/rights to execute the requested function at step 248 (also see Dustin Col. 18, lines 54-59). There is simply no teaching of retrieving a session data structure including a second credential and determining whether the (received) first credential matches this second credential. Rather, the cited reference teaches that the received *request* is compared to user permissions in a user table. This can be seen by at Dustan Col. 18, lines 54-65 where it states:

> "Assuming that the session id was found to be valid, decision step 238 proceeds to step 242 where the **function requested** by the user in the input **is compared** with the **user permissions or rights**, that, preferably, will be stored in the user table, to determine if the user has sufficient privileges or rights to execute the requested function. Also, step 242 involves comparing the current time to the last time that the user made a request during the current session. If this time is greater than a predefined period, such as fifteen minutes, an error message is provided to the client and the client is required to reenter the correct password. This is illustrated more fully in the following steps." (emphasis added by Appellants)

As Claim 22 also recites receiving a request (in addition to receiving a session identification and a first credential), the claimed first credential cannot reasonably be interpreted to be the Dustin request that is compared in step 248. Therefore, this permission determination at block 248 does not read on the claimed "determining whether the first credential and the second credential match", as the operation at Dustin step 248 uses the received *request* – which is different from Dustan's received session ID and account number - in the comparison. Thus, it is further shown that there is no teaching of retrieving a session data structure including a second credential in response to the session identification being valid, and determining whether the (received) first credential matches

this second credential. Therefore, Claim 22 (and thus Group I) is shown to not be anticipated by the cited reference as there is at least one missing claimed element.

B. Appellants will now show that the claims of Group II have been erroneously rejected under 35 U.S.C. 103(a) as the Examiner has failed to establish a prima facie case of obviousness with respect to the claims in Group II.

To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974). With respect to Claim 9, none of the cited references teach or suggest the claimed steps of "determining whether the credential is valid for ***both*** **the client and the session data**" or "sending the information to the client **in response to the session identification *and* the credential being valid**" (emphasis added). Nor has the Examiner alleged any such teaching or suggestion. In finally rejecting Claim 9, the Examiner states (paragraph 11 of Office Action dated 05/22/2003):

> "Dustan et al, figures 5 and 6, teach a system and method for securely accessing information from data sources through a network such that Applicants' step of sending a request reads on the menu selection at step 218, Applicants' credential reads on the account number and password at step 176, Applicants' session identification reads on step 216, Applicants' second request reads on step 234. Dustan et al fail to teach that associating the presented credential with session data. However, Shi et al teach associating the presented credential with session data in abstract, figs 1, 3 and column 3 lines 2-46. Therefore it would have been obvious to one of ordinary in the art at the time the invention was made to modify Dustan et al's inventive concept to include Shi et al's associating the presented credential with session data because this would have identifier to be used as a pointer into the in-memory credential database, and the credential is then retrieved and used to facilitate multiple file accesses from the distributed file system."

As can be seen from this reasoning in finally rejecting Claim 9, there is no allegation or other mention of any teaching or suggestion of "determining whether the credential is valid for ***both* the client and the session data**", or "sending the information to the client **in response to the session identification *and* the credential being valid**". Therefore, the Examiner has failed to establish a prima facie showing of obviousness. In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. Id. If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

The rejection of Claim 9 is thus shown to be improper, and should be overturned, as a prima facie case of obviousness has not been made by the Examiner. In addition, as a prima facie case of obviousness has not been made with respect to Claim 9, the burden has not shifted to Appellants to rebut an assertion of obviousness.

C. Appellants traverse the rejection of the claim in Group III by showing that no statutory basis has been given by the Examiner in rejecting this claim, yet its status is shown to be finally rejected on the Office Action Summary Page dated 05/22/2003 and the Advisory Action dated 09/03/2003. Per 35 U.S.C. 102, the language "A person shall be entitled to a patent *unless*-" (emphasis added by Appellants) places the initial burden on the Examiner in establishing a statutory basis for rejecting claims. It is not up to Appellants' to initially establish patentability of a claim. Thus, the Examiner has failed to properly reject the claim in Group III, as no statutory basis has been given in rejecting the claim in Group III.

In conclusion, Appellants respectfully request that the rejection of Claims 9-17, 22-29, 38-46, 51-58, 60, 62 and 63 be reversed by the Board for the reasons given above.

Duke W. Yee
Reg. No. 34,285

Wayne P. Bailey
Reg. No. 34,289
Carstens, Yee & Cahoon, LLP
PO Box 802334
Dallas, TX 75380
(972) 367-2001

APPENDIX OF CLAIMS

The text of the claims involved in the appeal are:

9. A method in a data processing system for managing an information request, comprising:

establishing a session, including authenticating a client based on a presented credential;

generating a session identification in response to the session being established;

associating the presented credential with session data;

sending the session identification to the client;

receiving a request for information and a credential and the session identification from the client;

determining whether the session identification is valid;

determining whether the credential is valid for both the client and the session data;

sending the information to the client in response to the session identification and the credential being valid.

10. The method of claim 9, wherein the credential is a user name and password, a security token, or a certificate.

11. The method of claim 9, further comprising:

associating a user account with the session identification in response to the credential being valid.

12. The method of claim 9, wherein the step of generating a session identification comprises generating a random number.

13. The method of claim 9, wherein the step of generating a session identification comprises generating a session identification data structure.

14. The method of claim 13, wherein the session identification data structure is a session identification cookie.

15. The method of claim 13, wherein the session identification data structure is in a rewritten uniform resource locator.

16. The method of claim 9, wherein the request is a hypertext transport protocol request.

17. The method of claim 16, wherein the hypertext transport protocol request is a uniform resource locator.

22. A method in a data processing system for managing an information request, comprising:

receiving a request for information and a session identification and a first credential from a client;

determining whether the session identification is valid;

retrieving a session data structure including a second credential in response to the session identification being valid;

determining whether the first credential and the second credential match; and

fulfilling the request for information in response to the first credential and the second credential matching.

23. The method of claim 22, wherein the first credential is a user name and password, a security token, or a certificate.

24. The method of claim 22, wherein the step of generating a session identification comprises generating a random number.

25. The method of claim 22, wherein the step of generating a session identification comprises generating a session identification data structure.

26. The method of claim 25, wherein the session identification data structure is a session identification cookie.

27. The method of claim 25, wherein the session identification data structure is in a rewritten uniform resource locator.

28. The method of claim 22, wherein the request is a hypertext transport protocol request.

29. The method of claim 28, wherein the hypertext transport protocol request is a uniform resource locator.

38. An apparatus for managing an information request, comprising:

session means for establishing a session, including authenticating a client based on a presented credential;

generating means for generating a session identification in response to the session being established;

association means for associating the presented credential with session data;

first sending means for sending the session identification to the client;

receipt means for receiving a request for information and a credential and the session identification from the client;

first determining means for determining whether the session identification is valid;

second determining means for determining whether the credential is valid for both the client and the session data; and

second sending means for sending the information to the client in response to the session identification and the credential being valid.

39. The apparatus of claim 38, wherein the credential is a user name and password, a security token, or a certificate.

40. The apparatus of claim 38, further comprising:

association means for associating a user account with the session identification in response to the session identification being generated.

41. The apparatus of claim 38, wherein the generating means comprises means for generating a random number.

42. The apparatus of claim 38, wherein the generating means comprises means for generating a session identification data structure.

43. The apparatus of claim 42, wherein the session identification data structure is a session identification cookie.

44. The apparatus of claim 42, wherein the session identification data structure is in a rewritten uniform resource locator.

45. The apparatus of claim 38, wherein the request is a hypertext transport protocol request.

46. The apparatus of claim 45, wherein the hypertext transport protocol request is a uniform resource locator.

51. An apparatus for managing an information request, comprising:

a processor; and

a memory electrically connected to the processor, the memory having stored therein a program to be executed on the processor for performing:

receiving a request for information and a session identification and a first credential from a client;

determining whether the session identification is valid;

retrieving a session data structure including a second credential in response to the session identification being valid;

determining whether the first credential and the second credential match; and

fulfilling the request for information in response to the first credential and the second credential matching.

52. The apparatus of claim 51, wherein the first credential is a user name and password, a security token, or a certificate.

53. The apparatus of claim 51, wherein the step of generating a session identification comprises generating a random number.

54. The apparatus of claim 51, wherein the step of generating a session identification comprises generating a session identification data structure.

55. The apparatus of claim 54, wherein the session identification data structure is a session identification cookie.

56. The apparatus of claim 54, wherein the session identification data structure is in a rewritten uniform resource locator.

57. The apparatus of claim 51, wherein the request is a hypertext transport protocol request.

58. The apparatus of claim 57, wherein the hypertext transport protocol request is a uniform resource locator.

60. A computer program product, in a computer readable medium, for managing an information request, comprising:

instructions for establishing a session, including authenticating a client based on a presented credential;

instructions for generating a session identification in response to the session being established;

instructions for associating the presented credential with session data;

instructions for sending the session identification to the client;

instructions for receiving a request for information and a credential and the session identification from a client;

instructions for determining whether the session identification is valid;

instructions for determining whether the credential is valid for both the client and the session data;

instructions for sending the information to the client in response to the session identification and the credential being valid.

62. A computer program product, in a computer readable medium, for managing an information request, comprising:

instructions for receiving a request for information and a session identification and a first credential from a client;

instructions for determining whether the session identification is valid;

instructions for retrieving a session data structure including a second credential in response to the session identification being valid;

instructions for determining whether the first credential and the second credential match; and

instructions for fulfilling the request for information in response to the first credential and the second credential matching.

63. A method in a data processing system for managing an information request, comprising:

authenticating a client based on a presented credential;

generating a session identification in response to the client being authenticated;

associating the presented credential with session data;

sending the session identification to the client;

receiving a request for information and a credential and the session identification from the client;

determining whether the session identification is valid;

determining whether the credential is valid for both the client and the session data; and

sending the information to the client in response to the session identification and the credential being valid.